CISION

ID: 95767971

VISÃO

04-11-2021

Meio: Imprensa
País: Portugal
Period.: Semanal
Âmbito: Interesse Geral

Pág: 78
Cores: Cor
Área: 18,00 x 27,00 cm²
Corte: 1 de 2

TECNOLOGIA

Vigiados no local de trabalho?

O uso de algoritmos que monitorizam, em tempo real, a atividade dos colaboradores está cada vez mais disseminado. O patrão está de olho – no escritório e no teletrabalho

CLARA SOARES

Quando navega na internet, no local de trabalho ou remotamente, é pouco provável que se questione sobre como são usados os sistemas de software da empresa em que desempenha funções. À partida, eles visam a segurança informática e seguem os protocolos previstos na lei. Ou talvez não? Desde que começou a pandemia, a oferta de produtos com recurso à Inteligência Artificial (IA) para monitorizar a atividade, on e offline, no meio laboral tem vindo a aumentar.

O propósito inicial era garantir a segurança, mas isso parece estar a mudar. No mercado, abundam serviços desenhados para aceder a indicadores de desempenho, em tempo real, com alertas que indicam alterações a determinada regra ou, até, para analisar dados pessoais dos colaboradores. Num artigo do jornal europeu *Politico*, referem-se situações que podem ter uma leitura dúbia. Por exemplo, o uso de pulseiras do pessoal das fábricas da Ford, com o argumento de garantir a distância social, ou a intenção da Amazon de recorrer à IA para monitorizar os movimentos dos funcionários de modo a minimizar o risco de doenças musculoesqueléticas. Em fevereiro, o gigante tecnológico instalou câmaras com indicadores biométricos para apurar quando é que os motoristas desviavam o olhar da estrada ou exce-

A AMAZON INSTALOU CÂMARAS COM INDICADORES BIOMÉTRICOS PARA APURAR QUANDO É QUE OS MOTORISTAS DESVIAVAM O OLHAR DA ESTRADA

CISION
ID: 95767971
VISÃO
04-11-2021
Meio: Imprensa
País: Portugal
Period.: Semanal
Âmbito: Interesse Geral
Pág: 79
Cores: Cor
Área: 18,00 x 27,00 cm²
Corte: 2 de 2

Uso ético da vigilância digital
Regulamentar os sistemas de IA é um desafio para a indústria e os decisores políticos

diam limites de velocidade, justificando que o fazia para reduzir acidentes.

Um relatório encomendado pela comissão de emprego do Parlamento Europeu revelou que "as tecnologias de vigilância reduzem a autonomia e a privacidade, conduzem a uma maior intensificação do trabalho e confundem as fronteiras entre o trabalho e a vida pessoal". Quem produz estes programas defende a sua dama. No artigo, Bradley Killinger, CEO da americana Sapience Analytics, afirmou que os seus produtos potenciavam o envolvimento, a produtividade e a satisfação com a carreira dos clientes e do pessoal da própria empresa, na qual, ao longo de seis semanas, houve funcionários a operar a 145% da capacidade. Onde fixar a linha vermelha no uso da Inteligência Artificial?

RISCO ELEVADO, MAIS CAUTELA

O que está em jogo, ao nível global, é a legitimidade dos fins que justificam os meios, ou seja, o uso ético desses meios. "Hoje, tudo é rastreável; monitorizar a atividade das pessoas será cada vez mais comum", esclarece Alípio Jorge, investigador do INESC TEC. O docente da Faculdade de Ciências da Universidade do Porto assume que a IA faz parte do nosso quotidiano e devemos estar conscientes disso: "Habituamo-nos à crescente algoritmização; usamos a Via Verde, fazemos compras online, mas temos de ter cautela e antecipar onde estão os riscos." O software de IA permite analisar grandes quantidades de dados, em tempo real, e pode ser uma mais-valia no meio laboral. "A geolocalização, os sistemas biométricos e os biossensores já são usados em profissões com elevado risco de stresse", mas sem regulamentação da vigilância digital no local de trabalho, as práticas abusivas são uma possibilidade real.

Há sete meses, a Comissão Europeia elaborou o AI Act, uma proposta para regulamentar estas tecnologias tendo em conta os riscos associados e as questões de ética e segurança, proibindo ou condicionando, em alguns casos, a utilização da IA. Por exemplo, os sistemas criados com a meta de processar dados em tempo real para fins de recrutamento e seleção, tomada de decisões (promoções, cessações de contratos de trabalho), avaliação do desempenho ou do comportamento são considerados aplicações de "risco elevado". Assim sendo, "os fornecedores podem precisar de uma certificação, para as pessoas não serem lesadas", frisa Alípio Jorge. Será suficiente? O investigador admite que "não conseguimos parar o rio, mas vamos ter de o gerir para não morrermos afogados", lema dirigido, também, a quem desenvolve e aplica IA.

Num mundo com cada vez mais procedimentos automatizados, o Regulamento Geral sobre a Proteção de Dados da União Europeia teve o mérito de acautelar direitos, ao "tornar a privacidade, obscurecida há dez anos, numa coisa real", afirma Vergílio Rocha, ex-diretor de sistemas de informação da EDP. O consultor lembra que isso é também evidente na Califórnia, na Austrália e no Reino Unido. As regras vão sendo implementadas, embora de modo imperfeito, dentro e fora da Europa. "Já não estamos na selva, mas o leão continua a prevalecer e a gazela só sobrevive se a polícia travar o leão", prossegue. "A lei foi aplicada pelas empresas, mas os casos que surgem, ciclicamente, na Imprensa, mostram que há dirigentes que não entendem as suas responsabilidades." A diferença é que, "hoje, estão sujeitas a coimas".

Foi o caso do banco britânico Barclays: após ser investigado pelos reguladores por vigiar os funcionários com recurso a ferramentas com IA, passou a anonimizar os dados rastreados. No setor do vestuário, a sueca H&M foi multada em Hamburgo, na Alemanha, por seguir perfis dos colaboradores e guardar registos de saúde e outros dados pessoais. Porém, ainda há muito a fazer para proteger os trabalhadores. "A UE perdeu a batalha com as grandes plataformas americanas, o AI Act ainda está na barriga da mãe", critica José Magalhães, membro do Conselho Superior de Segurança do Ciberespaço. Neste cenário, defende a adoção de medidas de autoproteção, como "acionar funções no browser que neutralizam mecanismos de monitorização e controlo". Lembrando a importância da nova lei do teletrabalho, cuja votação final no Parlamento está prevista para a próxima semana, o deputado acrescenta: "É preciso aprender a fazer guerrilha contra a vigilância abusiva ou ilegal e apresentar queixa à Comissão Nacional de Proteção de Dados (CNPD), para ver se fazem alguma coisa."

BOAS PRÁTICAS

Fatores "amigos" do uso responsável dos sistemas de Inteligência Artificial (IA) nas empresas

AVALIAÇÃO DE RISCOS
Criar mecanismos para prevenir, detetar e corrigir impactos negativos do software e eleger fornecedores que respeitam as disposições europeias

CULTURA ORGANIZACIONAL
Adotar sistemas de IA que se alinhem com os valores do negócio e os direitos das pessoas e recorrer, sempre que necessário, à intervenção humana

CULTIVAR A TRANSPARÊNCIA
Informar os colaboradores sobre a finalidade dos sistemas utilizados, dos filtros de segurança (palavras-chave, sites, ficheiros) aos programas de monitorização com IA

IA SIM, MAS COM ÉTICA

As recomendações da CNPD sobre o teletrabalho na pandemia apenas referem que as tecnologias de controlo remoto para rastrear páginas de internet, programas e ficheiros visualizados, monitorizar o que está no ambiente de trabalho ou o tempo gasto em cada tarefa (Time Doctor, Hubstaff ou Harvest, por exemplo) "recolhem manifestamente em excesso dados pessoais e não devem ser admitidos".

Ana Sofia Carvalho, membro do Grupo Europeu de Ética para a Ciência e a Tecnologia e docente do Instituto de Ciências Biomédicas Abel Salazar, no Porto, está entre os subscritores do Manifesto "Um compromisso nacional para uma transformação digital centrada no ser humano", apresentado, em março, pela Associação para a Promoção e Desenvolvimento da Sociedade da Informação, no qual constam grandes companhias, como a Google. "A regulamentação dos dispositivos com IA é um desafio para a indústria e os decisores políticos", conclui.

O complexo equilíbrio entre a vigilância digital e a privacidade só pode ser atingido conjugando o Código do Trabalho, boas práticas e literacia digital, ingredientes da confiança no meio corporativo. csoares@visao.pt